March 2nd, 2021

Try our March Fraud Prevention Quiz

This week's stories:

U.K. Launches Self-Assessment Tool and Awareness Campaign for Small Business Cybersecurity

Bespoke advice to help small businesses combat rising online threats is being offered through a new digital tool launched by the U.K.'s leading cybersecurity experts.

As part of the cross-government Cyber Aware campaign, GCHQ's National Cyber Security Centre (NCSC) has created the Cyber Action Plan to help micro businesses and sole traders securely navigate the increasingly digital landscape they operate in.

The U.K. government's most recent Cyber Security Breaches Survey found that almost half of micro and small businesses reported cybersecurity breaches or attacks in the past year. 46% were victims of these cyber incidents – up from 31% the previous year.

To help increase their digital defence, micro businesses and sole traders are being invited to complete a short questionnaire at www.cyberaware.gov.uk that generates a personalized list of actions linked to the Cyber Aware behaviors.

Over the past year some entrepreneurs have launched online-only businesses, following necessary restrictions to curb the spread of COVID-19. The Cyber Action Plan is a useful tool to help start-ups and other small businesses understand their online risk.

https://www.hstoday.us/industry/u-k-launches-self-assessment-tool-and-awareness-campaign-for-small-business-cybersecurity/

Click link above to read more

Why what you watch can make you a target for cybercriminals

Resist the lure of catching up with award nominees by trolling for free views. Free, when offered by bad actors, could end up costing you much more than it would for a one-time rental.

Free, more often than not, comes with strings. When it comes to movies and TV shows, treat "free" with a good deal of skepticism, according to new research from Kaspersky.

It's been a year since most people have been able to share a movie-going experience with an audience. But what's been devastating to the theater industry has been an unquestionable boon to streaming services. When the pandemic forced people indoors, they made good use of their subscription services.

Even if you have one or all of "the big three" Netflix, Hulu and Amazon Prime, you still won't be able to watch "Wandavision," "The Servant" or "The Mandalorian." What if you're compelled to see those shows and can't justify subscribing to the channel (i.e. Disney Plus, Apple TV)?

It might cheer you to see, with minimal research, that the shows are available to download for free. Unfortunately, you'll be sorely disappointed when you realize you've fallen victim to cybercrime.

https://www.techrepublic.com/article/why-what-you-watch-can-make-you-a-target-for-cybercriminals/

Click link above to read more

Suspicious finds: Researcher discovers Go typosquatting package that relays system information to Chinese tech firm

A Go package that relays system information to a Chinese IP address was one of several suspicious repositories uncovered during an investigation into typosquatting in the Go ecosystem.

Using a tool he built for the research project, GitLab security engineer Michael Henriksen scanned all 731 GitHub and GitLab hosted packages from the Go Module Index, surfacing seven dubious packages in all.

Typosquatting refers to malicious packages with near-identical names to those of legitimate packages, uploaded to repositories in the hope that developers will mistype the package name and inadvertently download the rogue version.

https://portswigger.net/daily-swig/suspicious-finds-researcher-discovers-go-typosquatting-package-that-relays-system-information-to-chinese-tech-firm

Click link above to read more

European e-ticketing platform Ticketcounter extorted in data breach

A Dutch e-Ticketing platform has suffered a data breach after a user database containing 1.9 million unique email addresses was stolen from an unsecured staging server.

Ticketcounter is a Dutch e-Ticketing platform that allows clients, such as zoos, parks, museums, and events, to provide online tickets to their venue.

On February 21st, a threat actor created a topic on a hacker forum to sell the stolen Ticketcounter database but quickly took the post down.

It was believed at first to be removed out of concern for the watchful eyes of the Netherlands Police. However, the threat actor told BleepingComputer that they have no fear of law enforcement, and they removed it as the database was sold privately.

From the samples of the database seen by BleepingComputer, the data exposed can include full names, email addresses, phone numbers, IP addresses, and hashed passwords.

https://www.bleepingcomputer.com/news/security/european-e-ticketing-platform-ticketcounter-extorted-in-data-breach/

Click link above to read more

Universities Face Double Threat of Ransomware, Data Breaches

Lack of strong security policies put many schools at risk of compromise, disrupted services, and collateral damage.

Institutions of higher education continue to have problematic password policies, lack multifactor authentication (MFA), and have a plethora of open ports — despite suffering dozens of ransomware attacks and targeting by attackers focused on stealing student information and university research, according to a new study published Tuesday.

An analysis by cybersecurity services firm BlueVoyant of publicly reported cybersecurity incidents involving higher education found that over the past two years, about 9% of the passwords on a common list used by attackers matched those used in combination with a university-assigned e-mail address. Meanwhile, about two-thirds of universities had no DNS-based e-mail security protocols in place, and 38% of all universities had at least one open database port.

https://www.darkreading.com/attacks-breaches/universities-face-double-threat-of-ransomware-data-breaches/d/d-id/1340242

Click link above to read more

Americans are at risk of being dragged into global cyber warfare, FireEye's CEO warns: 'It's as simple as if you can be hacked, you are hacked'

- Americans are at risk of being dragged into cyber warfare, FireEye's CEO told "Axios on HBO."
- Future cyberattacks could take down connected devices, leading to disruptions in daily life.
- "It's as simple as if you can be hacked, you are hacked," he said.

Americans are at risk of being dragged into cyber attacks that would put their connected devices at risk, according to the cybersecurity executive whose company discovered the SolarWinds hack.

Kevin Mandia, the CEO of cybersecurity company FireEye, told "Axios on HBO" on Sunday that future cyber warfare between the US and China or Russia could impact regular citizens, leading to widespread disruptions to daily life.

https://ca.news.yahoo.com/americans-risk-being-dragged-global-214230123.html

Click link above to read more

SolarWinds blames intern for weak passwords breach

Troubled software firm SolarWinds may have had more security issues than previously thought after admitting a severe security lapse in password protection.

During a court hearing into the company's failings that led to a major cyberattack affecting the likes of the US government and Microsoft, it was revealed that a password for a company file server was leaked and discovered online.

And in an embarrassing revelation for the company, the password was revealed to be the easily-guessable "solarwinds123".

In an apparent attempt to pass the buck, SolarWinds leadership past and present blamed the shortcomings on an unidentified intern, claiming that once spotted, the issue was corrected within days, but were roundly rebuked by US lawmakers overseeing the case.

https://www.techradar.com/news/solarwinds-blames-intern-for-weak-passwords-breach

Click link above to read more

VPNs still dominate post-COVID, but businesses are sniffing for alternatives

Virtual Private Networks have been around for decades, but over the past year many organizations were forced to expand their use to keep up with growing telework trends. In response, criminal and state-backed hacking groups have stepped up their own exploitation of the technology as well.

A recent report from Zscaler found that VPNs are still overwhelmingly popular: 93 percent of companies surveyed reported that they have used them in some capacity. The flip side of that coin is a similarly broad recognition of the dangers and tradeoffs involved, with 94 percent saying they are also aware of the security risks associated with using VPNs and two-thirds (67 percent) acknowledging that they are considering alternative options for secure remote access.

https://www.scmagazine.com/home/security-news/vpns-still-dominate-post-covid-but-businesses-are-sniffing-for-alternatives/

Click link above to read more

Far-Right Platform Gab Has Been Hacked—Including Private Data

The transparency group DDoSecrets says it will make the 70 GB of passwords, private posts, and more available to researchers, journalists, and social scientists.

WHEN TWITTER BANNED Donald Trump and a slew of other far-right users in January, many of them became digital refugees, migrating to sites like Parler and Gab to find a home that wouldn't moderate their hate speech and disinformation. Days later, Parler was hacked, and then it was dropped by Amazon web hosting, knocking the site offline. Now Gab, which inherited some of Parler's displaced users, has been badly hacked too. An enormous trove of its contents has been stolen—including what appears to be passwords and private communications.

On Sunday night the WikiLeaks-style group Distributed Denial of Secrets is revealing what it calls GabLeaks, a collection of more than 70 gigabytes of Gab data representing more than 40 million posts. DDoSecrets says a hacktivist who self-identifies as "JaXpArO and My Little Anonymous Revival Project" siphoned that data out of Gab's backend databases in an effort to expose the platform's largely right-wing users. Those Gab patrons, whose numbers have swelled after Parler went offline, include large numbers of Qanon conspiracy theorists, white nationalists, and promoters of former president Donald Trump's election-stealing conspiracies that resulted in the January 6 riot on Capitol Hill.

https://www.wired.com/story/gab-hack-data-breach-ddosecrets/

Click link above to read more

Flaws fixed incorrectly, as secure coding education lags

Broken access control and broken object level authorizations vulnerabilities have proven the most difficult to fix, while fixes for command injection and SQL injection flaws are most often incorrect.

Research released from HackEDU, which was based on feedback from primarily security, development and compliance leaders, attributed the failures to a lack of formal training, with about 53 percent of developers not trained on secure coding practices.

“The data comes from the assessments, lessons, the challenges and the actual reported vulnerabilities from HackEDU customers and students,” Brandon Hoe, head of marketing at HackEDU told SC Media.

The report noted that command injection vulnerabilities can be prevented by simply “adhering to the principle of never calling out to OS commands from application layer code; however developers often try to fix them with insufficient filters.”

https://www.scmagazine.com/home/patch-management/flaws-fixed-incorrectly-as-secure-coding-education-lags/

Click link above to read more

How to manage the security challenges triggered by remote work

Remote employees have engaged in certain risky behaviors, such as storing sensitive data, using inappropriate admin access and failing to update software, says Tanium.

The coronavirus pandemic forced organizations to quickly and unexpectedly shift employees to a remote working environment. Though many IT teams have handled the transition as effectively as possible, such an abrupt change has still opened the door for increased security risks. A report released Monday by security provider Tanium examines some of the threats facing organizations with a remote work scenario and offers tips on how to manage them.

Entitled "IT Leads the Way: How the Pandemic Empowered IT," the new report is based on a survey of IT decision makers across 500 different enterprise companies. Conducted by research firm PSB Insights on behalf of Tanium, the survey elicited responses from a variety of sectors in the U.S. and the U.K., with more than half of the respondents C-level decision-makers.

In early 2020, 88% of those surveyed expressed some level of confidence in their ability to fully and securely support a remote workforce. Yet after the pandemic hit, 61% of the respondents admitted that they had difficulty switching to a work-from-home environment. As a result, 73% said they now face new IT security challenges, while 52% acknowledged that their security challenges have become more complex.

https://www.techrepublic.com/article/how-to-manage-the-security-challenges-triggered-by-remote-work/

Click link above to read more

Malware Loader Abuses Google SEO to Expand Payload Delivery

Gootloader has expanded its payloads beyond the Gootkit malware family, using Google SEO poisoning to gain traction.

The Gootloader malware loader, previously used for distributing the Gootkit malware family, has undergone what researchers call a “renaissance” when it comes to payload delivery.

New research released this week paints Gootloader as an increasingly sophisticated loader framework, which has now expanded the number of payloads its delivers beyond Gootkit (and in some cases, the

previously-distributed REvil ransomware), to include the Kronos trojan and the Cobalt Strike commodity malware.

Gootloader is known for its multi-stage attack process, obfuscation tactics, and for using a known tactic for malware delivery called search engine optimization (SEO) poisoning. This technique leverages SEO-friendly terms in attacker-controlled websites, in order to rank them higher in Google's search index. In the end, the method brings more eyeballs to the malicious sites, which contain links that launch the Gootloader attack chain.

https://threatpost.com/malware-loader-google-seo-payload/164377/

Click link above to read more

How stalkerware can threaten your safety and privacy, and how to avoid it

With a stalkerware app on your phone, another person can spy on your activities and view your personal information, Kaspersky says.

At its best, technology can bring people together through the use of social networks, video chats, and other tools. But at its worst, technology can be used to harass, bully, and terrorize other people. One example of the latter is stalkerware, a type of app installed on someone's mobile device to eavesdrop on them. A report released Friday by Kaspersky explains how stalkerware works and how you can protect yourself against it.

Commercially available to anyone with internet access, stalkerware typically is set up on someone's mobile phone without their knowledge or permission. Once installed, the app operates in stealth mode, so the user is unaware of its presence.

https://www.techrepublic.com/article/how-stalkerware-can-threaten-your-safety-and-privacy-and-how-to-avoid-it/

Click link above to read more

Offboarding: A Checklist for Safely Closing an Employee's Digital Doors

Three years after I left my former job, I got an official letter telling me the organization suffered a data breach. My personal information was at risk of identity theft. I shouldn't have been surprised. That job's offboarding process hadn't been the best. For years after leaving, I had access to my email and to databases filled with sensitive data. While the cause of this data breach was never revealed, it could have very well been a former employee with a grudge, someone who had the same easy access I did.

The employee offboarding policy and process is usually handled by human resources and the employee's bosses. Maybe legal gets involved if there is something nefarious happening. IT and cybersecurity are an afterthought, if decision-makers even consider them at all. Even if you take away the former employee's physical access — the keys, the badge — they may still be able to log in to the network, putting the company at risk of data breaches and putting them in violation of privacy compliance.

Before an employee goes through the final offboarding process with HR, IT and security teams should begin the process of deleting the out-going employee from network access.

https://securityintelligence.com/articles/offboarding-checklist-safely-closing-doors/

Click link above to read more

Hackers release a new jailbreak tool for almost every iPhone | TechCrunch

An iPhone hacking team has released a new jailbreak tool for almost every iPhone, including the most recent models, by using the same vulnerability that Apple last month said was under active attack by hackers.

The Unc0ver team released its latest jailbreak this weekend, and says it works on iOS 11 (iPhone 5s and later) to iOS 14.3, which Apple released in December.

Jailbreaking is a cat-and-mouse game between security researchers who want greater control and customizations over their phones, and Apple, which says it locks down iPhones for security. Hackers build jailbreak tools by finding and exploiting vulnerabilities that can lift some of the restrictions that Apple puts in place, like installing apps outside of its app store, which most Android users are already used to.

https://techcrunch.com/2021/03/01/hackers-unc0ver-jailbreak-iphone/?guccounter=1

Click link above to read more

Private information of thousands who received Covid vaccine exposed in HSE blunder

Major details that can be used to allow access to financial, health and highly personal files online were left exposed

The private information of thousands of people who have received the Covid-19 vaccine have been exposed following a HSE blunder.

The IT system used by the HSE was compromised due to 'human error', meaning that confidential data was accessible despite earlier warnings by data chiefs.

Crucial details that can often be used to certify access to financial, health and highly personal files online were left exposed, including PPS numbers, addresses, names and contact details.

https://www.irishmirror.ie/news/irish-news/health-news/private-information-thousands-who-received-23566568

Click link above to read more

AOL Phishing scam threatens to close account

Attackers have been targeting AOL users in an attempt to steal login name and password with a phishing link. Many older people are still using AOL, because they find it too complicated to switch to a different email service such as Gmail or Outlook. This makes them prime targets for phishing scams, especially as AOL's email filters are not as efficient as those from other services.

https://www.itsecurityguru.org/2021/03/01/aol-phishing-scam-threatens-to-close-account/?utm_source=rss&utm_medium=rss&utm_campaign=aol-phishing-scam-threatens-to-close-account

Click link above to read more

---

http://www2.gov.bc.ca/gov/content/governments/services-for-government/information-management-technology/information-security/security-news-digest

To learn more about information security issues and best practices, visit us at:

https://www.gov.bc.ca/informationsecurity

OCIOSecurity@gov.bc.ca